AF

TRANSMITTAL OF APPEAL BRIEF

Docket No. SMY-219.01

Applicant:	Stephen R. Hanna and Radia J. Perlman
Serial No:	09/517,410
Filed:	March 2, 2000
For:	METHOD AND APPARATUS FOR USING NON-SECURE FILE SERVERS FOR SECURE INFORMATION STORAGE
Examiner:	J. R. Adams
Art Unit:	2134

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Mail Stop Appeal Brief - Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 on May 16, 2005.

Jan L. Mellen

Jan L. Mellen

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Transmitted herewith is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on February 16, 2005.

Status of Applicant

This application is on behalf of Sun Microsystems, Inc..

☐ Applicant claims small entity status.

Extension of Time

☒ The proceedings herein are for a patent application and the provisions of 37 C.F.R.1.136 apply. An extension of time of 1 months is requested.

Fee Due

Appeal Brief Fee	500.00
Extension of Time Fee	120.00
TOTAL FEE	620.00

Payment

☒ Enclosed is a check in the amount of the total fee.

☐ The Commissioner is authorized to charge the total fee to Deposit Account No. 02-3038.

☒ The Commissioner is hereby authorized to charge any other fees under 37 C.F.R. §1.16 and §1.17 that may be required, or credit any overpayment, to Deposit Account No. 02-3038. A duplicate of this transmittal letter is attached.

Paul E. Kudirka Date: 5/16/05

Paul E. Kudirka, Esq. Reg. No. 26,931
KUDIRKA & JOBSE, LLP
Customer Number 045774
Tel: (617) 367-4600 Fax: (617) 367-4656

APPEAL BRIEF UNDER 37 CFR §41.37	Docket No. SMY-219.01

Applicant:	Stephen R. Hanna and Radia J. Perlman
Serial No:	09/517,410
Filed:	March 2, 2000
For:	METHOD AND APPARATUS FOR USING NON-SECURE FILE SERVERS FOR SECURE INFORMATION STORAGE
Examiner:	J. R. Adams
Art Unit:	2134

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Mail Stop Appeal Brief - Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 on May 16, 2005.

Jan L. Mellen

Jan L. Mellen

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This brief is in furtherance of the Notice of Appeal, filed in this case on February 16, 2005.

The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

A single copy of this brief is transmitted (37 C.F.R. 41.37(a)) and contains these items under the following headings, and in the order set forth below (37 C.F.R. 41.37(c)(1)):

I REAL PARTY IN INTEREST (37 C.F.R. 41.37(c)(1)(i))

The real party in interest in this appeal is Sun Microsystems, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. 41.37(c)(1)(ii))

There are no other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this pending appeal.

III STATUS OF CLAIMS (37 C.F.R. 41.37(c)(1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1, 4-10, 12, 13 and 15-37.

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims pending: 1, 4-10, 12, 13 and 15-37
2. Claims canceled: 2, 3, 11 and 14.
3. Claims withdrawn from consideration, but not canceled: none.
4. Claims allowed: none.
5. Claims rejected: 1, 4-10, 12, 13 and 15-37.

C. CLAIMS ON APPEAL

The claims on appeal are: 1, 4-10, 12, 13 and 15-37.

IV STATUS OF AMENDMENTS (37 C.F.R. 41.37(c)(1)(iv))

A Response to Final Office Action was filed on October 18, 2004 and was entered, but did not place the application in condition for allowance. A Supplemental Amendment After Final Action was filed on January 7, 2005, but the status of this latter amendment is unclear, since no response has been received regarding it.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. 41.37(c)(1)(v))

The claimed invention in the present application is a system and method for transmitting information from a client 12 to a file server 14 and storing that information on the file server, where the information is secret and both the file server and the mechanism for transmitting the information from the client to the file server are not secure (Page 1, lines 23-25). According to the claimed technique, the information is first encrypted at the client with a first encryption key (step 22, Figure 5). A decryption key that allows the information encrypted with the first key to be decoded is then encrypted at the client with a second key known to the client (step 24). The encrypted key is then associated with a client ID (step 26). Then, the encrypted information, the encrypted key and the client ID are sent to the file server (step 28). At the file server 14, the

encrypted information is stored and the encrypted key is stored in an access control list (Figures 3a and 4a) that contains a client ID identifying the client, the encrypted key and information identifying where the information is stored (Page 9, lines 17-23).

The use of an access control list allows other parties to access the information even if they did not store the information on the file server in the first place as long as they can obtain the second key. In order to allow another party to access the information, the client that stored the information in the first place retrieves the access control list, and obtains the decryption key by using the second key (known to it) to decrypt the first key (step 40, Figure 6). Then the first key is encrypted with an additional ID for the new member (step 42) and associated with an additional new member ID (step 44) and added to the access control list (step 46). See Page 11, lines 1-17)

When someone requests the information from the file server 14, they send their ID to the file server 14 along with a request for data. The server 14 receives the request (step 60, Figure 7) then looks up the ID in the access control list and retrieves the data and the encrypted first key (step 62). The file server 14 returns the encrypted data and the encrypted first key to the requester (step 64). When a requesting client receives the information and the encrypted key (step 82, Figure 8), it decrypts the encrypted first key (step 84) and then uses it to decrypt the encrypted information (step 86). See Page 11, line 17- page 12, line 6.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. 41.37(c)(1)(vi))

Claims 1, 4-7 and 13-18 stand rejected as obvious over the combination of U.S. Patent No. 5,748,735 (Ganesan) and U.S. Patent No. 5,495,533 (Linehan). Claims 31-34 stand rejected as anticipated by Ganesan and claims 35-37 stand rejected as anticipated by Linehan. Claims 8-11 stand rejected as obvious over the combination of Ganesan and Linehan in view of page 364 of "Handbook of Applied Cryptography", A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, CRC Press 1997 (Menezes). Claim 12 stands rejected as obvious over the combination of Ganesan, .Linehan, Menezes and U.S. Patent No. 5,787,175 (Carter). Claim 20 stands rejected as obvious over the combination of Linehan and U.S. Patent No. 5,787,169 (Eldridge.) Claims 21-30 stand rejected as obvious over the combination of Ganesan and Eldridge.

VII ARGUMENT (37 C.F.R. 41.37(c)(1)(vii))

The Ganesan reference does not anticipate claims 31-34.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

First, it should be noted that, in accordance with the invention as claimed, both encryption and decryption of the information is performed at the client. The client also generates the first and second keys so that no key server is necessary. All information passing to and from the file server, including the information itself and any keys necessary to decrypt that information, is encrypted. The retrieval operation is clearly recited in claim 31. Claim 31 recites in response to an information retrieval request, "receiving from said file server said information encrypted with a first encryption key having an associated first decryption key ..." and an "entry associated with a client authorized to at least read said information, ...including said first decryption key encrypted with a second encryption key having an associated second decryption key ...that is accessible to said client "

This is in contrast to the arrangement disclosed in Ganesan. In Ganesan, the client and the server first exchange encrypted requests for the stored information (steps 500 - 570, Figure 5) to insure that the request is from the proper party. Then the server retrieves an encrypted crypto-key and encrypted data from storage (580). Note that the crypto-key has been encrypted with an encryption key that is known to the server, not the client. Thus, the server decrypts this crypto-key key using is own private key (585). The server uses the crypto-key to decrypt the information (590) and then sends the plaintext information to the client (595.) Thus, Ganesan does not disclose that the client receives from the server "...said information encrypted with a first encryption key having an associated first decryption key ..." as recited in claim 31. The examiner merely states that Ganesan does disclose transmitting encrypted data from the file server to the client, but it is clear from the Ganesan disclosure that this does not happen. Further, the client does not receive a "first decryption key encrypted with a second encryption key having an associated second decryption key ...that is accessible to said client "also as recited in claim 31. In Ganesan, such a key is not necessary since the data has already been decrypted at the server. Thus, claim 31 patentably distinguishes over the Ganesan reference. Claims 32-34 are dependent on claim 31 and incorporate the limitations thereof. Therefore, they distinguish over the cited Ganesan reference in the same manner as claim 31.

The Linehan reference does not anticipate claims 35-37.

The Linehan reference discloses a method for securely storing encrypted data. Linehan uses both a key server and a file server. When a client wants to store a file on the file server it sends an ID (a "ticket" as described in Linehan) to the key server together with the file name. The key server then generates an encryption key, stores the key and file name and sends the key back to the client. The client then encrypts the information with the key and sends the encrypted information to the file server where it is stored. Thus, the unencrypted key is stored on the key server and the encrypted data is stored in the file server. This arrangement differs from that recited in claim 35. Claim 35 recites program code for storing on the file server "information encrypted with a first encryption key having a corresponding first decryption key that is usable to decrypt said encrypted information " and an entry including "said first decryption key encrypted with a second encryption key associated with one of a plurality of clients authorized to at least read said information " In Linehan, the key used to encrypt the information stored on the file server is not stored in encrypted form, either in the file server as recited or in the key server of Linehan. Linehan does suggest that the encryption key could be transmitted to the client encrypted with a *session* key (column 8, lines 20-23.) However, the information encryption as encrypted with the session key is clearly not stored on the file server with the information as recited in claim 35 or, for that matter, on the key server. Thus, claim 35 patentably distinguishes over the cited Linehan reference. Claims 36-37 are dependent on claim 35 and incorporate the limitations thereof. Therefore, they distinguish over the cited Linehan reference in the same manner as claim 35.

Prima facie obviousness has not been established because the combination of Ganesan and Linehan is not proper and does not teach or suggest the structure recited in claims 1, 4-7 and 13-18.

Obviousness is a legal conclusion based on factual evidence. Graham v. John Deere Co. 383 US 1, 148 USPQ 459 (1966). The PTO has the burden under section 103 to establish a prima facie case of obviousness. In re Piasecki, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787-87 (Fed. Cir. 1984). To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1970.)

a. The combination of Ganesan and Linehan is improper

If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention, being modified, then the teachings of the reference are not sufficient to render the claims prima facie obvious. In re Ratti, 46 C.C.P.A. 976, 270 F.2d 810, 123 USPQ 349 (CCPA 1959.)

Ganesan and Linehan operate in a completely different fashion. For example, as mentioned above, in Ganesan, file encryption is performed at the file server, whereas in Linehan, file encryption is performed at the client. This difference results in different keys being stored in different locations and different keys being used for encryption and decryption. Thus, to combine these references it would be necessary to redesign one of the systems to use the keys and operation of the other reference. This redesign is impermissible.

b. The combination of Ganesan and Linehan does not teach or suggest the combination clamed in claims 1, 4-7 and 13-18.

Even assuming that the Ganesan and Linehan references could and should be combined, the resulting combination cannot teach or suggest the claimed invention. For example, claim 1 is representative. It recites storing at the file server "(i) information encrypted with a first encryption key and (ii) ... an entry that includes an identifier for a client authorized to at least read said encrypted information and a first decryption key encrypted with a second encryption key ...that is accessible to the client." As noted above, Ganesan stores the file encryption key at the file server encrypted with a key that is accessible to the file server, not the client. Linehan does not store the encrypted file encryption key (presumably, the key server is secure). Since, neither reference discloses the claimed limitation, the combination cannot teach or suggest the combination. Claims 4-7 depend on claim 1 and incorporate the limitations thereof. Therefore, they distinguish over the cited combination of the Ganesan and Linehan references in the same manner as claim 1. Claim 13 contains limitations that parallel those in claim 1 and thus distinguishes over the cited combination of references in the same manner as claim 1. Claims 14-18 depend on claim 13 and incorporate the limitations thereof. Therefore, they distinguish over the cited combination of the Ganesan and Linehan references in the same manner as claim 13. Thus, claims 1, 4-7 and 13-18 patentably distinguish over the cited combination of references.

Prima facie obviousness has not been established because the combination of Ganesan, Linehan and Menezes does not teach or suggest the structure recited in claims 8-11.

The Menezes reference is a page from a general handbook on cryptography. Thus, its incorporation into the combination of Ganesan and Linehan cannot change the basic operation of the Ganesan and Linehan combination that is discussed above. Claims 8-11 are dependent on claim 1 and incorporate its limitations. Since, as set forth above, the Ganesan and Linehan combination does not teach or suggest the limitations of claim 1, adding Menezes to the combination cannot create the required teaching or suggestion.

Prima facie obviousness has not been established because the combination of Ganesan, Linehan, Menezes and Carter does not teach or suggest the structure recited in claim 12.

Carter discloses a method and apparatus for controlling collaborative access to a work group document by the users of a computer system. The document has an encrypted data portion and a prefix portion. Data structures in the prefix portion are used to restrict access to the information stored in the data portion. However, in Carter users do not access the data over unsecure communication links. Thus, Carter is not concerned with passing plaintext information over those links. Consequently, Carter, as Ganesan performs encryption and decryption of the data at the server. Thus, its addition cannot change the basic operation of the Ganesan, Linehan and Menezes combination. Claim 12 depends indirectly on claim 1 and incorporates its limitations. Since the Ganesan, Linehan and Menezes combination does not teach or suggest the limitations of claim 1, adding Carter to the combination cannot create the required teaching or suggestion.

Prima facie obviousness has not been established because the combination of Eldridge and Linehan does not teach or suggest the structure recited in claim 20.

The Eldridge reference is similar to the Carter reference in that users do not access the data over unsecure communication links. Thus, Eldridge is not concerned with passing plaintext information over those links. Consequently, Eldridge, as Linehan performs encryption and decryption of the data at the server. Thus, its addition cannot change the basic operation of Linehan. Claim 20 contains limitations that parallel those in claim 1. Since Linehan does not teach or suggest the limitations of claim 1 as discussed above, adding Eldridge to the combination cannot create the required teaching or suggestion.

Prima facie obviousness has not been established because the combination of Eldridge and Ganesan does not teach or suggest the structure recited in claims 21-30.

As mentioned above, the Eldridge system discloses performing encryption and decryption of the data at the server. Thus, its addition to Ganesan cannot change the basic operation of Ganesan. Claim 21 contains limitations that parallel those in claim 1. Since Ganesan does not teach or suggest the limitations of claim 1 as discussed above, adding Eldridge to the combination cannot create the required teaching or suggestion. The remainding claims 22-30 dependent on claim 21 and therefore distinguish over the cited combination in the same manner as claim 21.

VIII APPENDIX OF CLAIMS (37 C.F.R. 41.37(c)(1)(viii))

The text of the claims involved in the appeal is:

1. A method of operation at a file server, the method comprising:

storing (i) information encrypted with a first encryption key and (ii) an access control list usable by said file server to control access to said encrypted information, said access control list including an entry that includes an identifier for a client authorized to at least read said encrypted information and a first decryption key encrypted with a second encryption key, wherein said first decryption key is usable to decrypt said encrypted information, and wherein said second encryption key is associated with a second decryption key that is usable to decrypt said encrypted first decryption key and that is accessible to said client, and

in response to a request from said client; transmitting to said client said encrypted information and said entry.

4. The method of claim I wherein transmitting comprises transmitting to said client said access control list.

5. The method of claim 1 wherein said first encryption key and said first decryption key are symmetric.

6. The method of claim 1 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and said first decryption key comprises the other of said public key and said private key of said first public/private key pair.

7. The method of claim 1 wherein said identifier includes one of an unencrypted identifier and an encrypted identifier.

8. The method of claim 1 wherein said entry includes said first decryption key combined with a check value to form a data stream, wherein said data stream is encrypted with said second encryption key; and

transmitting comprises transmitting to said client said encrypted information and said access control list.

9. The method of claim 8 wherein said check value comprises a value known to said client.

10. The method of claim 8 wherein said check value comprises said client identifier.

12. The method of claim 8 wherein said check value comprises a group identifier that identifies a group of which said client is a member.

13. A method for securely storing information on a file server and distributing the stored information, said method comprising:

encrypting information at one of a plurality of clients in communication with said file server, said information being encrypted with a first encryption key having an associated first decryption key that is usable to decrypt said encrypted information;

encrypting said first decryption key with a second encryption key for each of said plurality of clients authorized to at least read said information, wherein each respective

one of said second encryption keys has a corresponding second decryption key that is usable to decrypt said respective encrypted first decryption key and that is retained by the respective one of said plurality of clients;

storing said encrypted information on said file server and storing on said file server said encrypted first decryption keys as a plurality of entries within an access control list, wherein each one of said entries is associated with one of said plurality of clients;

forwarding to at least a selected one of said plurality of clients said encrypted information and at least one of said entries in response to a request received at said file server from said selected one of said plurality of clients;

decrypting said encrypted first decryption key contained in said at least one of said entries utilizing the second decryption key corresponding to the second encryption key for the respective entry; and

decrypting said encrypted information using said first decryption key to obtain said information.

15. The method of claim 13 wherein said request includes a client identifier associated with said selected one of said plurality of clients, said entries each include a client identifier associated with one of said plurality of clients, and wherein forwarding includes forwarding to at least said selected one of said plurality of clients the entry including the client identifier that is associated with the client identifier contained within said request.

16. The method of claim 13 wherein forwarding comprises forwarding to said selected one of said plurality of clients said encrypted information and said access control list.

17. The method of claim 13 wherein said first encryption and decryption keys are symmetric.

18. The method of claim 13 wherein said second encryption and decryption keys are symmetric.

19. The method of claim 13 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and the first decryption key comprises the other of said public key and said private key of said first public/private key pair.

20. A method for storing information securely on a file server for access by members of a group, said method comprising:

identifying the members of said group, wherein said group has a group identifier,

encrypting information with a first encryption key having an associated first decryption key that is usable to decrypt said encrypted information;

encrypting said first decryption key with a group encryption key having an associated group decryption key for decrypting data encrypted with said group encryption key;

storing said encrypted information on said file server and storing said encrypted first decryption key on said file server within an access control list associated with said encrypted information and containing, at least at some times, a plurality of encrypted first decryption keys, and

in response to a request received at said file server from one of said members of said group, forwarding to said one of said members of said group said encrypted information and at least said first decryption key encrypted with said group encryption key.

21. A method for accessing information securely stored on a file server for access by members of a group, said method comprising:

identifying the members of said group, wherein said group has a group identifier,

encrypting information with a first encryption key having an associated first decryption key that is usable to decrypt said encrypted information;

encrypting said first decryption key with a group encryption key having an associated group decryption key for decrypting data encrypted with said group encryption key;

storing said encrypted information on said file server and storing said encrypted first decryption key on said file server within an access control list associated with said encrypted information and containing, at least at some times, a plurality of encrypted first decryption keys;

in response to a request received at said file server from one of said members of said group, forwarding to said one of said members of said group said encrypted information and at least said encrypted first decryption key encrypted with said group encryption key;

in a first decrypting, decrypting said encrypted first decryption key with said group decryption key to obtain said first decryption key; and

in a second decrypting, decrypting said encrypted information using said first decryption key to obtain said information.

22. The method of claim 21 wherein said method further includes distributing said group decryption key to said members of said group and said first decrypting comprises decrypting the encrypted first decryption key by said one of said members of said group using the distributed group decryption key.

23. The method of claim 21 wherein said first decrypting comprises:

forwarding said encrypted first decryption key to a group server associated with said group identifier;

decrypting said encrypted first decryption key at said group server using said group decryption key; and

forwarding said first decryption key to said one of said group members.

24. The method of claim 23 wherein forwarding said first decryption key to said one of said group members comprises forwarding the first decryption key to said one of said group members over a secure channel.

25. The method of claim 24 wherein said secure channel is a physically secure channel.

26. The method of claim 24 wherein said secure channel comprises a non-secure communications path and forwarding the first decryption key to said one of said group members over a secure channel comprises:

encrypting said first decryption key with a third encryption key having an associated third decryption key known to said one of said group members;

forwarding to said one of said group members said encrypted first decryption key encrypted with said third encryption key; and

decrypting by said one of said group members, said encrypted first decryption key encrypted with said third encryption key using said third decryption key.

27. The method of claim 26 wherein said third encryption key comprises a public key of a member public/private key pair and wherein said third decryption key comprises the member private key of said member public/private key pair.

28. The method of claim 26 wherein said third encryption and decryption keys are symmetric.

29. The method of claim 21 wherein said first encryption and decryption keys are symmetric.

30. The method of claim 21 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and the first decryption key comprises the other of said public key and said private key of said first public/private key pair.

31. A method for accessing information stored securely on a file server, the method comprising:

forwarding to said file server a request for information from a client;

in response to said request, receiving from said file server said information encrypted with a first encryption key having an associated first decryption key that is usable to decrypt said encrypted information and at least one access control list entry associated with a client authorized to at least read said information, said received at least one entry including said first decryption key encrypted with a second encryption key having an associated second decryption key that is usable to decrypt said encrypted first decryption key and that is accessible to said client;

decrypting said encrypted first decryption key using said second decryption key to obtain said first decryption key; and

decrypting said encrypted information using said first decryption key.

32. The method of claim 31 wherein said first encryption and decryption keys are symmetric.

33. The method of claim 31 wherein said first encryption key comprises one of a public key and a private key of a first public/private key pair and the first decryption key comprises the other of said public key and said private key of said first public/private key pair.

34. The method of claim 31 wherein said second encryption key comprises a public key of a member public/private key pair and said second decryption key comprises the private key of said member public/private key pair.

35. A computer program product including a computer readable medium, said computer readable medium having a file server computer program stored thereon, said file server computer program for execution in a computer and comprising:

program code for storing on said file server information encrypted with a first encryption key having a corresponding first decryption key that is usable to decrypt said encrypted information;

program code for storing on said file server an access control list, said access control list including at least one entry, said at least one entry including said first decryption key encrypted with a second encryption key associated with one of a plurality of clients authorized to at least read said information and having access to a second decryption key associated with said second encryption key and usable to decrypt said encrypted first decryption key; and

program code for transmitting to said one of said plurality of clients said encrypted information and said at least one entry.

36. A computer data signal, said computer data signal including a computer program for use in accessing encrypted information stored on a file server, said computer program comprising:

program code for storing on said file server information encrypted with a first encryption key having a corresponding first decryption key that is usable to decrypt said encrypted information;

program code for storing on said file server an access control list, said access control list including at least one entry, said at least one entry including said first

decryption key encrypted with a second encryption key associated with one of a plurality of clients authorized to at least read said information and having access to a second decryption key associated with said second encryption key and usable to decrypt said encrypted first decryption key; and

program code for transmitting to said one of said plurality of clients said encrypted information and said at least one entry.

37. Apparatus for accessing encrypted data stored on a file server, the apparatus comprising:

means for storing on said file server information encrypted with a first encryption key having a corresponding first decryption key that is usable to decrypt said encrypted information;

means for storing on said file server an access control list, said access control list including at least one entry, said at least one entry including said first decryption key encrypted with a second encryption key associated with one of a plurality of clients authorized to at least read said information and having access to a second decryption key associated with said second encryption key that is usable to decrypt said encrypted first decryption key; and

program code for transmitting to said one of said plurality of clients said encrypted information and said at least one entry.

Respectfully submitted

Paul E. Kudirka Date: 5/16/05

Paul E. Kudirka, Esq. Reg. No. 26,931
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656